

# A Motivated Account of Hilbert's Proof of His Irreducibility Theorem

Mark Villarino

Escuela de Matemática  
Universidad de Costa Rica

William Gasarch

Department of Computer Science  
University of Maryland

Kenneth W. Regan

Department of Computer Science and Engineering  
University at Buffalo (SUNY)

January 18, 2017

## Abstract

Hilbert's Irreducibility Theorem is a cornerstone that joins areas of analysis and number theory. Both the genesis and genius of its proof involved combining real analysis and combinatorics. We try to expose the motivations that led Hilbert to this synthesis. Hilbert's famous Cube Lemma supplied fuel for the proof but without the analytical foundation and framework it would have been heating empty air. The lemma is said to presage Ramsey Theory but we note differences in motivation.

## 1 Introduction

In 1892, David Hilbert published a proof of the following theorem, known today as *Hilbert's Irreducibility Theorem*, which he stated as follows.

**Theorem 1.** *If  $F(x, y, \dots, w; t, r, \dots, q)$  is an irreducible polynomial with integral coefficients<sup>1</sup> in the variables  $x, y, \dots, w$  and the parameters  $t, r, \dots, q$ , then it is always possible, and indeed in infinitely many ways, to substitute integers for the parameters  $t, r, \dots, q$  such that the polynomial  $F(x, y, \dots, w; t, r, \dots, q)$  becomes an irreducible polynomial in the variables  $x, y, \dots, w$ , alone.*

To Hilbert, this theorem was not an end in itself but rather a tool to use for some remarkable applications. A simple one is that if a polynomial  $f(x)$  over  $\mathbf{Z}$  has values that are perfect squares for all sufficiently large  $x$ , then  $f(x)$  must be the square of some other polynomial over  $\mathbf{Z}$ . One of his most striking ones is:

---

<sup>1</sup>A polynomial in any number of variables whose coefficients are integers will be called an *integral* polynomial. [Hilbert's footnote]

**Corollary 2.** *For every integer  $n$  there exist infinitely many polynomials  $p$  in  $\mathbf{Z}[x]$  such that  $p$  has the symmetric group  $S_n$  as its Galois group.*

He began his paper [13] with a statement and proof of the two-variable case, which is the fundamental step in the proof of the general theorem. Again in Hilbert’s own words, the statement is:

**Theorem 3.** *If  $f(x, t)$  is an irreducible polynomial in the two variables  $x$  and  $t$  with integral coefficients*

$$f(x, t) = Tx^n + T_1x^{n-1} + \cdots + T_n,$$

*where  $T, T_1, \dots, T_n$  are integral polynomials in  $t$ , it is always possible, indeed in infinitely many ways, to substitute an integer for  $t$  in  $f(x, t)$  such that the polynomial  $f(x, t)$  becomes an irreducible polynomial of the single variable  $x$ .*

A more modern formulation is:

**Theorem 4.** *Let  $f(x, y) \in \mathbf{Z}[x, y]$  be irreducible. For an infinite number of  $t \in \mathbf{Z}$ ,  $f(x, t)$  (as an element of  $\mathbf{Z}[x]$ ) is irreducible.*

In fact, Hilbert proved the *contrapositive*, which can be formulated as follows.

**Theorem 5.** *Let  $f(x, y) \in \mathbf{Z}[x, y]$ . If there exists  $t_0$  such that for every integer  $t \geq t_0$ ,  $f(x, t)$  is reducible over  $\mathbf{Z}$ , then  $f(x, y)$  is reducible over  $\mathbf{Z}$ .*

Hilbert proved this by formulating what is today called *Hilbert’s Cube Lemma*. It can be viewed not only as an enhanced form of Dirichlet’s pigeonhole principle but also as the first statement of a Ramsey-type theorem. Our next section gives a Ramsey-style statement in terms of “colors” and a brief modern proof. It is easy to appraise this as a gem in an isolated setting and forget the quest that led to it, which was *to find a polynomial factor*,  $\varphi(x, t) \in \mathbf{Z}[x, t]$ , of the polynomial  $f(x, t)$ .

The *motivation* for the lemma is our purpose here. We provide a motivated account of Hilbert’s beautiful proof of (ir)reducibility by putting ourselves in his shoes and following the trail of ideas that we find in his 1892 paper. We have tried to make it self-contained for readers at roughly third-year mathematics undergraduate level.

## 2 The Cube Lemma

Hilbert’s first paragraph crisply framed the *problem* of irreducibility under substitutions represented by the statement of Theorem 1. Then he continued right away, “Our developments rest on the following lemma.” We reproduce his words but change his  $a, \mu$  to  $c, \beta$  and compact his displayed formulas using 0–1 variables  $b_1, \dots, b_m$ :

“Given an infinite integer sequence  $a_1, a_2, a_3, \dots$  in which generally each  $a_s$  denotes one of the  $c$ -many positive integers  $1, 2, \dots, c$ , let  $m$  be any positive whole number. Then there are always  $m$ -many positive whole numbers  $\mu^{(1)}, \mu^{(2)}, \dots, \mu^{(m)}$  such that the  $2^m$  elements

$$a_{\beta + \sum_{i=1}^m b_i \mu^{(i)}}$$

for infinitely many whole numbers  $\beta$  are collectively the same number  $G$ , where  $G$  is one of the numbers  $1, 2, \dots, c$ .”

Call those elements collectively the  $m$ -cube, which we can denote by  $C(\beta; \mu_1, \dots, \mu_m)$ . The sequence  $a_1, a_2, a_3, \dots$  can be called a *coloring* of  $\mathbf{N}^+$  using  $c$  colors. Thus the conclusion is that every coloring gives rise to *increments*  $\mu^{(1)}, \mu^{(2)}, \dots, \mu^{(m)}$  that yield a monochromatic  $m$ -cube for infinitely many starting points  $\beta$ . This is implied by the following finitistic statement, which we regard as **Hilbert’s Cube Lemma** in the modern sense:

**Lemma 6.**

*For all  $m, c$  there is a number  $H$  such that, for all  $c$ -colorings of  $\mathbf{N}^+$  and all intervals of length  $H$  in  $\mathbf{N}^+$ , there is a monochromatic  $m$ -cube within the interval.*

The following proof tries to be simplest; we discuss optimizations and Hilbert’s original proof in Section 12 at the end.

*Proof.* The proof is by induction on  $m$ . For the base case  $m = 1$ , we can take  $H_1 = c + 1$ . This just says that for any  $c$ -coloring of an interval of length  $c + 1$  there will be two elements that are the same color. Taking  $\beta$  to be the smaller one and  $\beta + \mu_1$  the larger one,  $C(\beta; \mu_1)$  is a monochromatic 1-cube.

For the induction, assume that  $h = H_{m-1}$  exists. We show that, for any  $c$ -coloring of an interval of length  $H_m = h \cdot (1 + c^h)$ , there is a monochromatic  $m$ -cube. Let  $COL$  be a  $c$ -coloring of an interval of length  $H_m$ . Partition the interval into  $1 + c^h$  blocks of size  $h$ . By the pigeonhole principle, some two of those blocks have the same sequence of  $h$  colors. By the induction hypothesis, the former has a monochromatic  $(m - 1)$ -cube  $C(\beta; \mu_1, \dots, \mu_{m-1})$ , and since the color sequence of the latter is the same, it has  $C(\beta'; \mu_1, \dots, \mu_{m-1})$  with the same color and increments but  $\beta' > \beta$ . Take  $\mu_m = \beta' - \beta$ . Then  $C(\beta; \mu_1, \dots, \mu_m)$  is the required monochromatic  $m$ -cube. ■

A common form of Ramsey’s Theorem [21] states that for all  $c$  and  $m$  there is a number  $R = R(m, c)$  such that all  $c$ -colorings of the edges of the complete graph on  $R$  nodes contain a monochromatic clique of at least  $m$  nodes. More generally, Ramsey Theory deals with coloring objects (e.g., edges of graphs, sets of numbers) and getting nice monochromatic subsets. According to Graham–Rothschild–Spencer [9], Landman–Robertson [15], Promel [20] and

Soifer [25], the Hilbert Cube Lemma is the first ever “Ramseyan” theorem proven. Hilbert, however, viewed his lemma as a means to an end and did not launch what is now called Ramsey Theory. We discuss this matter further at the end after presenting the motivations we find in Hilbert’s paper.

After Hilbert, many mathematicians offered other proofs of the Irreducibility Theorem. Dorge [4] proved it without using the Cube Lemma. Lang [16, 17] and Prasolov [19] have expositions of this proof. Franz [6] also gave a proof that does not use the Cube Lemma, and this is expounded further by Schinzel [23]. There is another alternative proof by Fried [7]. Many of these proofs use so-called “density” arguments, a standard technique in today’s Diophantine approximation theory, but a far cry from the natural idea of Hilbert to find a factor of a reducible polynomial. We will say more about modern proofs in Section 11.

Hilbert remains one of the greatest mathematicians of all time. His original proof still contains insights and arguments that are well worth study even today. We offer the reader a detailed exposition of this proof in hope of saving it from the oblivion of history.

### 3 Monic Polynomials and Gauss’s Polynomial Lemma

Hilbert begins by reducing his general problem to the case of *monic polynomials in one variable*  $x$  with *rational* coefficients. That is, by means of the substitution  $x = \frac{y}{T}$  we obtain

$$f(x, t) = \frac{1}{T^{n-1}} \{y^n + S_1 y^{n-1} + S_2 y^{n-2} + \cdots + S_n\},$$

where  $S_1, S_2, \dots, S_n$  again are certain integral polynomials in  $t$ , and therefore *the polynomial*

$$g(y, t) = y^n + S_1 y^{n-1} + S_2 y^{n-2} + \cdots + S_n$$

*becomes reducible for every positive integral value of  $t$  that exceeds a certain limit  $C' \geq C$ .* Moreover,  $t$  can be chosen so large that the polynomial  $T$  remains different from zero for all values of  $t$  exceeding  $C'$ .

**Proposition 7.** *If  $g(y, t)$  is reducible over  $\mathbf{Q}[y, t]$ , then  $f(x, t)$  is reducible over  $\mathbf{Z}[x, t]$ .*

In order to prove this, we must preface the following lemma:

**Lemma 8.** *Let  $f(x, y) \in \mathbf{Z}[x, y]$  and  $g(x, y) \in \mathbf{Z}[x, y]$  and suppose that they are arranged according to powers of  $x$ :*

$$\begin{aligned} f(x, y) &= a_0(y)x^n + a_1(y)x^{n-1} + \cdots + a_{n-1}(y)x + a_n(y), \\ g(x, y) &= b_0(y)x^n + b_1(y)x^{n-1} + \cdots + b_{n-1}(y)x + b_n(y), \end{aligned}$$

*where each  $a_i$  and  $b_i$  belongs to  $\mathbf{Z}[y]$ . Then:*

- (a) *A necessary and sufficient condition that a polynomial  $\psi(y)$  be a factor of  $f(x, y)$  is that it is a factor of all the polynomials  $a_i(y)$ .*

- (b) If  $\psi(y)$  is irreducible and divides the product  $f \cdot g$  then either it is a factor of all  $a_i(y)$  or a factor of all  $b_i(y)$ .
- (c) If  $f(x, y)$  can be factored into the product of two polynomials in  $x$  whose coefficients are rational functions of  $y$  with integral coefficients, i.e., in  $\mathbf{Z}[x](y)$ , then it can be factored into the product of two polynomials in  $\mathbf{Z}[x, y]$ .

*Proof.* Statements (a) and (b) are straightforward and well-known; see Bôcher [1, pp. 203–204], for example. To prove statement (c), we write the given factorization in the form

$$f(x, y) = \frac{f_1(x, y)}{\varphi_1(y)} \cdot \frac{f_2(x, y)}{\varphi_2(y)},$$

where  $f_1(x, y)$ ,  $f_2(x, y)$ ,  $\varphi_1(y)$  and  $\varphi_2(y)$  are integral polynomials such that  $f_1$  is not divisible by any factor of  $\varphi_1(y)$  and  $f_2$  is not divisible by any factor of  $\varphi_2(y)$ . By part (b), since  $f_1 \cdot f_2$  is divisible by  $\varphi_1 \cdot \varphi_2$ ,  $f_1$  has the complete polynomial  $\varphi_2$  as a factor and  $f_2$  has the complete polynomial  $\varphi_1$  as a factor. By (a) we can cancel  $\varphi_2$  from the coefficients of  $f_1$  and we can cancel  $\varphi_1$  from the coefficients of  $f_2$ . This gives us our factorization into two polynomials in  $\mathbf{Z}[x, y]$ . ■

*Proof of the reducibility of  $f(x, t)$  over  $\mathbf{Z}[x, t]$ .* By hypothesis,

$$g(y, t) = \Psi(y, t)\Psi'(y, t),$$

where  $\Psi(y, t) \in \mathbf{Q}[x, t]$  and  $\Psi'(y, t) \in \mathbf{Q}[x, t]$ . where  $\Psi(y, t)$  and  $\Psi'(y, t)$  belong to  $\mathbf{Q}[y, t]$ . By means of the substitution  $y = xT$  we obtain the following equation for our original polynomial:

$$f(x, t) = \frac{\Phi(x, t)\Phi'(x, t)}{AT^{n-1}},$$

where  $\Phi(x, t) \in \mathbf{Z}[x, t]$  and  $\Phi'(x, t) \in \mathbf{Z}[x, t]$ , while  $A \in \mathbf{Z}$  and  $T \in \mathbf{Z}[t]$ . Now part (c) of our lemma completes the proof. ■

So the whole proof of Theorem 5 (and hence Theorems 3 and 1) boils down to showing that *if for almost all  $t \in \mathbf{Z}$ ,  $g(x, t)$  is reducible over  $\mathbf{Z}[x]$ , then  $g(x, y)$  is reducible over  $\mathbf{Q}[x, y]$ .*

Proposition 7 is a two-variable variant of an important and famous result that algebraists call *Gauss's Lemma for Polynomials*. The one-variable case that appears in paragraph 42 of Gauss's *Disquisitiones* [8] is as follows:

*The product of two monic polynomials over the rationals with at least one rational non-integral coefficient is itself a monic polynomial over the rationals with at least one rational non-integral coefficient.*

The modern version follows at a stroke upon observing that if even one of its factors has a non-integral coefficient, so does the original reducible integral polynomial, a contradiction:

*If a monic integral polynomial is reducible over the rational numbers, then its polynomial factors are themselves integral polynomials.*

We know of no occurrences of Gauss's version in literature outside the *Disquisitiones*, yet all proofs of the modern statement are modeled on Gauss's original proof, as here. Gauss used his lemma to give the first proof of the irreducibility of the cyclotomic polynomial of prime degree over the rationals. As we've seen above, Hilbert uses it to reduce the Irreducibility Theorem to the case of monic polynomials with rational coefficients.

## 4 Puiseux Series

The fundamental theorem of algebra shows us that the equation  $g(y, t) = 0$  has  $n$  complex roots for each value of  $t$ . Thus, informally, there are  $n$  functions of  $t$ , say  $y_1(t), \dots, y_n(t)$ , which satisfy the equation. Hilbert uses a refined form of the *implicit function theorem*, which we refer to as *Puiseux's theorem* (see discussion of origins below). It says that the  $n$  root functions  $y_1(t), \dots, y_n(t)$  can be expressed in a concrete way by means of fractional power series in decreasing powers of the variable. These are the so-called *Puiseux series at infinity*, whose definition we now recall.

**Definition 1.** *Let  $m \in \mathbf{N}$ . A Puiseux series at infinity is an expression of the form*

$$u(x^{1/k}) + \sum_{i=1}^{\infty} \frac{B_i}{x^{i/k}},$$

where  $u(x) \in \mathbf{C}[x]$  is of degree  $m$ ,  $k \in \mathbf{N}^+$ , and  $B_1, B_2, \dots \in \mathbf{C}$ .

We adopt the following theorem statement from [27, pp. 80–81] with slight alterations in notation and formatting. The power series in (1) are called *Puiseux expansions at infinity*.

**Theorem 9 (Puiseux's Theorem).** *Given  $g(y, t)$  as above, there is a finite Galois extension  $K/\mathbb{Q}$ , which we view as a subfield of  $\mathbb{C}$ , and  $n$  distinct formal power series*

$$\begin{aligned} y_1(t) &= A_{11}\tau^h + A_{12}\tau^{h-1} + \dots + A_{1,h+1} + \frac{B_{11}}{\tau} + \frac{B_{12}}{\tau^2} + \frac{B_{13}}{\tau^3} + \dots \\ y_2(t) &= A_{21}\tau^h + A_{22}\tau^{h-1} + \dots + A_{2,h+1} + \frac{B_{21}}{\tau} + \frac{B_{22}}{\tau^2} + \frac{B_{23}}{\tau^3} + \dots \\ &\vdots \\ y_n(t) &= A_{n1}\tau^h + A_{n2}\tau^{h-1} + \dots + A_{n,h+1} + \frac{B_{n1}}{\tau} + \frac{B_{n2}}{\tau^2} + \frac{B_{n3}}{\tau^3} + \dots \end{aligned} \tag{1}$$

where the following hold:

- (a) For a certain positive integer  $k$ ,  $\tau = t^{1/k}$ , where the positive real value of the root is meant;

- (b) *The given number  $h$  is the highest positive exponent of  $\tau$  that occurs.*
- (c) *All coefficients  $A_{i,j}$  and  $B_{i,j}$  belong to  $K$ ;*
- (d) *Any formal power series  $y(t)$  satisfying the formal identity  $g\{y(t), t\} \equiv 0$  and having properties analogous to those of the series (1), even without the requirement that the coefficients of  $y(t)$  be algebraic, necessarily coincides with one of the above  $n$  series*
- (e) *We have the formal identity:*

$$g(y, t) \equiv \prod_{i=1}^n \{y - y_i(t)\}.$$

- (f) *Each series (1) converges for  $|t| > B_0$ , where  $B_0$  is the maximum modulus of the roots of the resultant polynomial  $\text{Res}_y(g, \frac{\partial g}{\partial y}) \in \mathbb{Z}[t]$ .*
- (g) *For each  $i$  the function  $\tau \mapsto y_i(\tau^{-k})$  is analytic and one-to-one into the punctured disk with center at the origin and radius  $B_0^{-1/k}$ . ■*

Hilbert ascribed the idea he used to Runge in a work that had appeared three years earlier, and cited it in a footnote exactly like this.<sup>2</sup> He then notes—and this is the reason to reduce the problem to monic polynomials—the relation between the elementary symmetric functions of the roots  $y_1, y_2, \dots, y_n$  and the coefficient polynomials  $S_1, S_2, \dots, S_n$ , namely:

$$\begin{aligned} S_1 &= -(y_1 + y_2 + \dots + y_n) \\ S_2 &= (-1)^2(y_1 y_2 + y_1 y_3 + \dots + y_{n-1} y_n) \\ &\vdots \\ S_n &= (-1)^n(y_1 y_2 y_3 \dots y_{n-1} y_n). \end{aligned} \tag{2}$$

The insight is that by Puiseux's Theorem, when we plug the expansions (1) into the symmetric functions (2), *the resulting fractional power series for the coefficients all collapse down to the integral polynomials  $S_k$  in  $t$ .*

We formulate this simple observation as a theorem, calling the part of the expansion with positive exponents the *polynomial part*.

**Theorem 10.** *For any  $g(x, y) \in \mathbf{C}[x, y]$  the elementary symmetric functions of  $n$  Puiseux expansions (1) collapse down to polynomials in  $\mathbf{Z}[t]$  if and only if:*

- (a) *The coefficients of all the negative powers of  $\tau$  in the resulting fractional power series for the coefficients are **all equal to zero**.*

---

<sup>2</sup>The original work of Puiseux can be found in *Liouville's Journal*, vols. 15, 16 (1850, 1851). These expansions have already been used by *C. Runge* to derive necessary conditions that an equation between two unknowns have infinitely many integral solutions. See this Journal, vol. 100, p. 425. [Hilbert's footnote]

- (b) *The numerical coefficients of the “polynomial part” of the resulting fractional power series for the coefficients **are all integers**.*
- (c) *The numerical coefficients of the positive non-integral fractional powers of  $\tau$  in the resulting fractional power series for the coefficients are **all equal to zero**.* ■

These three conditions will, with appropriate changes, characterize the coefficients of *any polynomial factor in  $\mathbf{Z}[y, t]$  of  $g(y, t)$* . Lemma 8 above shows that we can write “*rational numbers*” instead of “*integers*” in condition (b).

## 5 The Formal Factors

Any *formal* polynomial factor of  $g(y, t)$  is a polynomial of the form

$$\pi_A(y, t) := \prod_{y_j \in A} (y - y_j), \quad (3)$$

where  $A$  is a subset of the roots  $\{y_1, y_2, \dots, y_n\}$ . As Hilbert points out, there are  $\binom{n}{2}$  quadratic factors,  $\binom{n}{3}$  cubic factors,  $\binom{n}{4}$  quartic factors,  $\binom{n}{5}$  quintic factors, and so on, and finally  $\binom{n}{n-1}$  factors of degree  $n - 1$ . Additionally, we count the  $n$  linear factors for a grand total of

$$\binom{n}{2} + \binom{n}{3} + \dots + \binom{n}{n-1} + n = 2^n - 2$$

possible factors. So, if  $g(y, t)$  is reducible, *some  $\pi_A(y, t)$ , must be an integral polynomial factor*. We assign to each set  $A$  a unique index  $a$  where  $a = 1, 2, \dots, 2^n - 2$ . And by abuse of notation we call  $\pi_A(y, t)$  by the name  $\pi_a(y, t)$  where  $a$  is the unique index assigned to  $A$ .

Let’s look at a simple example of a reducible integral polynomial:

$$g(y, t) := y^3 - t^3.$$

Then the roots of  $g(y, t) = 0$  are  $y_1 = t$ ,  $y_2 = \omega t$ ,  $y_3 = \omega^2 t$  where  $\omega^3 = 1$ ,  $\omega \neq 1$ .<sup>3</sup> When  $n = 3$  there are  $2^3 - 2 = 6$  formal factors. Thus the sets  $A$  are

$$\{y_1\}, \quad \{y_2\}, \quad \{y_3\}, \quad \{y_1, y_2\}, \quad \{y_1, y_3\}, \quad \{y_2, y_3\},$$

and we (arbitrarily) assign the indices  $a = 1, 2, 3, 4, 5, 6$  to them respectively. Then, by (3) these formal factors are:

$$\begin{aligned} \pi_{\{y_1\}} &\equiv \pi_1(y, t) = y - y_1 = y - t, \\ \pi_{\{y_2\}} &\equiv \pi_2(y, t) = y - y_2 = y - \omega t, \\ \pi_{\{y_3\}} &\equiv \pi_3(y, t) = y - y_3 = y - \omega^2 t, \\ \pi_{\{y_1, y_2\}} &\equiv \pi_4(y, t) = (y - y_1)(y - y_2) = y^2 + \omega t y + \omega^2 t^2, \\ \pi_{\{y_1, y_3\}} &\equiv \pi_5(y, t) = (y - y_1)(y - y_3) = y^2 + \omega^2 t y + \omega t^2, \\ \pi_{\{y_2, y_3\}} &\equiv \pi_6(y, t) = (y - y_2)(y - y_3) = y^2 + t y + t^2. \end{aligned}$$

---

<sup>3</sup>Moreover,  $y_1 = t$ ,  $y_2 = \omega t$ ,  $y_3 = \omega^2 t$  where  $\omega^3 = 1$ ,  $\omega \neq 1$  are also the Puiseux expansions of the roots.



We observe that  $\pi_1(y, t)$  and  $\pi_6(y, t)$  are *integral* polynomial factors whereas the other four are not.

## 6 Using the Pigeonhole Principle

Our problem, now, is to discover *which* formal factor  $\pi_\alpha$  is an *integral* polynomial. We begin our search by applying our hypothesis.

Let  $t_0$  be an integer greater than  $C'''$ , and let  $\tau_0$  be the positive  $k$ -th root of  $t_0$ . In general,  $\tau_0$  will be irrational. By hypothesis, if we substitute  $\tau_0$  into all of the coefficient series of the formal factors  $\pi_a(y, t)$ , *at least one of them will be an integral polynomial in  $y$ .*

Now, with Hilbert, we observe that if we substitute  $2\tau_0$  into all of the coefficient series of the formal factors  $\pi_a(y, t)$ , then *at least one of them will be an integral polynomial in  $y$* , by the assumption that  $g(y, 2^k t_0)$  is reducible.

Again, if we substitute  $3\tau_0$  into all of the coefficient series of the formal factors  $\pi_a(y, t)$  *at least one of them will be an integral polynomial in  $y$* , by the assumption that  $g(y, 3^k t_0)$  is reducible. The same is true of  $4\tau_0$ ,  $5\tau_0$ , and indeed, of  $\sigma\tau_0$  for  $\sigma = 1, 2, 3, \dots$

Therefore, we obtain *an infinite sequence of integral polynomial factors  $\pi_a(y, \sigma^k t_0)$  in  $y$ .* Each of them has a unique index  $a$  where  $a = 1, 2, \dots, 2^n - 2$ . Let these indices be  $a_1, a_2, a_3, \dots, a_s, \dots$ . Then, by the pigeonhole principle, *at least one index  $a_s$  occurs infinitely often.* In our example above, we can take  $a_s = 1$  or  $a_s = 6$  and our sequence of indices contains either 1 or 6 or both infinitely often. The point is that:

The corresponding formal polynomial  $\pi_{a_s}(y, t)$  is a natural candidate for our integral polynomial factor.

To prove that it *is* our integral polynomial factor, we must verify that its Puiseux series satisfy the three conditions of Theorem 10. The rest of Hilbert's paper (and ours) is the proof that the candidate formal factor  $\pi_{a_s}(y, t)$  satisfies the three conditions stated.

## 7 Framing the Cube Lemma

Let's consider the first condition: *The coefficients of all the negative powers of  $\tau_0$  in the resulting fractional power series for the coefficients of  $\pi_{a_s}(y, (\sigma^k t_0))$  are all equal to zero.* Suppose the following system of coefficient power series for  $\pi_{a_s}(y, (\sigma^k t_0))$  has  $a_s$  as its index:

$$\begin{aligned} y_1 + y_2 + \dots + y_\nu &= A_{11}(\sigma\tau_0)^h + A_{12}(\sigma\tau_0)^{h-1} + \dots + A_{1,h+1} + \frac{B_{11}}{\sigma\tau_0} + \frac{B_{12}}{(\sigma\tau_0)^2} + \frac{B_{13}}{(\sigma\tau_0)^3} + \dots \\ &\vdots \qquad \qquad \qquad \vdots \\ y_1 y_2 \dots y_\nu &= A_{\nu 1}(\sigma\tau_0)^{h\nu} + A_{\nu 2}(\sigma\tau_0)^{h\nu-1} + \dots + A_{\nu, h\nu+1} + \frac{B_{\nu 1}}{\sigma\tau_0} + \frac{B_{\nu 2}}{(\sigma\tau_0)^2} + \frac{B_{\nu 3}}{(\sigma\tau_0)^3} + \dots \end{aligned}$$

The coefficients  $A, B$  are all completely determinate rational or irrational, real or complex numbers; some of them have the value zero since the positive exponents of  $\tau_0$  in general will be smaller than  $(n - 1)h$ .

The variable quantity here is the integer  $\sigma$ . This suggests that *we rewrite the above fractional series as series in  $\sigma$  and then obtain:*

$$\begin{aligned} y_1 + y_2 + \cdots + y_\nu &= A_{11}\sigma^h + A_{12}\sigma^{h-1} + \cdots + A_{1,h+1} + \frac{B_{11}}{\sigma} + \frac{B_{12}}{\sigma^2} + \frac{B_{13}}{\sigma^3} + \cdots \\ &\vdots \qquad \qquad \qquad \vdots \\ y_1 y_2 \cdots y_\nu &= A_{\nu 1}\sigma^{h\nu} + A_{\nu 2}\sigma^{h\nu-1} + \cdots + A_{\nu,h\nu+1} + \frac{B_{\nu 1}}{\sigma} + \frac{B_{\nu 2}}{\sigma^2} + \frac{B_{\nu 3}}{\sigma^3} + \cdots \end{aligned}$$

where the new coefficients  $A, B$  are again determinate numerical quantities. Suppose that the index of the first occurrence of our infinitely repeated polynomial factor is  $s = \sigma = \mu$ . Then every repetition of the index  $\mu$  produces the same  $\nu$  power series in  $\sigma$ , but with a *larger* value of  $\sigma$ . Thus, since there are an infinite number of such indices,  *$\sigma$  tends to infinity in the above power series.*

If we look at the series of *negative* powers for any particular coefficient, we see that for sufficiently large  $\sigma$  it become arbitrarily small in absolute value. Yet, the total power series takes integral values for all of these values of  $\sigma$ . That suggests that the total contribution of the negative powers, for large  $\sigma$ , *is an integer of arbitrarily small absolute value, i.e., zero.*

Thus we might try to argue by contradiction as follows: assume that there *are* nonzero coefficients of negative powers and deduce an absurd conclusion. The possible hitch is that this inference ignores the “polynomial part” of the coefficient series—which could exactly compensate for a tiny non-zero contribution of the negative powers.

To show that this is *not* the case we would like to somehow “eliminate” the polynomial part of the coefficient series without losing the property of being an integer for infinitely many values of  $\sigma$ . This suggests *forming suitable linear combinations of the coefficient series which successively subtract off the principal terms of the polynomial parts, and leaving finally only linear combinations of integer-valued series with negative coefficients.*

To see how this would work, let’s look at a typical coefficient series. Let us choose any of the  $\nu$  power series in the system under consideration, say the power series

$$\mathcal{P}(\sigma) = A_{11}\sigma^{m-1} + A_{12}\sigma^{m-2} + \cdots + A_{1m} + \frac{B_{11}}{\sigma} + \frac{B_{12}}{\sigma^2} + \frac{B_{13}}{\sigma^3} + \cdots$$

where we have written  $m - 1$  for the highest power of  $\sigma$ .

Now comes a new insight. *This is the insight that is key to the whole proof.* Its simplicity belies the brilliance it took to think of it. Professional mathematicians are aware of this phenomenon: the deepest ideas, in the end, are based on a simple observation. Here is Hilbert’s. He began by extending his supposition:

Suppose that the series  $\mathcal{P}(\sigma)$  takes on integral values, not only for infinitely many values of  $\sigma$ , *but also for all the infinitely many values of  $\sigma + \mu^{(1)}$ , where  $\mu^{(1)}$  is a fixed increment independent of  $\sigma$ .*

Carrying forward, we can form the linear combination

$$\mathcal{P}^{(1)}(\sigma) := \mathcal{P}(\sigma) - \mathcal{P}(\sigma + \mu^{(1)})$$

and put the polynomial part equal to

$$\varphi_{m-1}(\sigma) := A_{11}\sigma^{m-1} + A_{12}\sigma^{m-2} + \cdots + A_{1m}$$

for brevity. We now start the argument-for-contradiction.

Suppose now that the other coefficients  $B_{11}, B_{12}, B_{13}, \dots$  of the power series  $\mathcal{P}(\sigma)$  are *not all zero* and let  $\frac{B_{1v}}{\sigma^v}$  be the first term whose coefficient  $B_{1v}$  does *not* vanish. Then

$$\mathcal{P}^{(1)}(\sigma) = \varphi_{m-1}(\sigma) - \varphi_{m-1}(\sigma + \mu^{(1)}) + B_{1v} \left[ \frac{1}{\sigma^v} - \frac{1}{(\sigma + \mu^{(1)})^v} \right] + \cdots$$

Here the first difference on the right hand side *is a polynomial of degree  $m - 2$  in  $\sigma$* ; we put

$$\varphi_{m-2}(\sigma) = \varphi_{m-1}(\sigma) - \varphi_{m-1}(\sigma + \mu^{(1)}).$$

We expand the remaining terms on the right hand side in decreasing powers of  $\sigma$ ; then we obtain<sup>4</sup>

$$\mathcal{P}^{(1)}(\sigma) = \varphi_{m-2}(\sigma) + \mu^{(1)v} \frac{B_{1v}}{\sigma^{v+1}} + \cdots$$

Now comes the upshot of Hilbert's insight:

*We have reduced the maximum degree of the polynomial part by one unit. Moreover,  $\mathcal{P}^{(1)}(\sigma)$  takes on integral values for infinitely many  $\sigma$ .*

This argument has *not yet* proved that such an increment  $\mu^{(1)}$  exists, but shows that if we could, then we could make a first step in reaching our goal of producing a series of negative powers of  $\sigma$  which is an integer for infinitely many values of  $\sigma$ .

---

<sup>4</sup>The details, with simplified notation, are:

$$\begin{aligned} B_{1v} \left[ \frac{1}{\sigma^v} - \frac{1}{(\sigma + \mu)^\nu} \right] &= \frac{B_{1v}}{\sigma^\nu} \left[ 1 - \frac{1}{(1 + \frac{\mu}{\sigma})^\nu} \right] \\ &= \frac{B_{1v}}{\sigma^\nu} \left[ 1 - \left\{ 1 + \binom{-\nu}{1} \frac{\mu}{\sigma} + \binom{-\nu}{2} \left( \frac{\mu}{\sigma} \right)^2 + \cdots \right\} \right] \\ &= \frac{B_{1v}}{\sigma^\nu} \left[ \frac{\mu\nu}{\sigma} - \frac{\nu(\nu+1)}{2} \left( \frac{\mu}{\sigma} \right)^2 + \cdots \right] \\ &= \frac{\mu\nu B_{1v}}{\sigma^{\nu+1}} \left[ 1 - \frac{\nu+1}{2} \left( \frac{\mu}{\sigma} \right) + \cdots \right], \end{aligned}$$

and this last expression on the right hand side is equivalent to that in the main body of the paper.

To carry out a similar program to *reduce the maximum degree of the polynomial part to  $m - 3$ , then to  $m - 4$ , and so on until finally to zero*, we would have to have to prove the existence of  $m$  fixed increments  $\mu^{(k)}$ ,  $k = 1, 2, \dots, m$  whose values are all independent of  $\sigma$  and such that if we substitute any of the integers:

$\mu$					
$\mu + \mu^{(1)}$					
$\mu + \mu^{(2)}$	$\mu + \mu^{(1)} + \mu^{(2)}$				
$\mu + \mu^{(3)}$	$\mu + \mu^{(1)} + \mu^{(3)}$	$\mu + \mu^{(2)} + \mu^{(3)}$	$\mu + \mu^{(1)} + \mu^{(2)} + \mu^{(3)}$		
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\dots$	$\ddots$
$\mu + \mu^{(m)}$	$\mu + \mu^{(1)} + \mu^{(m)}$	$\mu + \mu^{(2)} + \mu^{(m)}$	$\dots$	$\dots$	$\mu + \mu^{(1)} + \dots + \mu^{(m)}$

for  $\sigma$  in  $\mathcal{P}(\sigma)$ , the values will all be integers.

Note that the proof of the existence of the increment  $\mu^{(1)}$  amounts to proving that  $a_\mu$  and  $a_{\mu+\mu^{(1)}}$  are both *the same number in the set of indices  $a_s$* . A similar property holds for the set of all the above sums of fixed increments  $\mu^{(k)}$  (for  $k = 1, 2, \dots, m$ ) with  $\mu$ , namely that they all are the subscripts of *the same number in the set of indices  $a_s$* . In our running example they are all equal to 1 or they are all equal to 6.

The proof of the existence of these increments is the content of the *Hilbert Cube Lemma*. We now state it using his formulas much as he visualized them in his paper:

**Theorem 11.** *Let  $a_1, a_2, a_3, \dots$  be an infinite sequence in which the general term,  $a_s$ , is one of the  $a$  positive numbers  $1, 2, \dots, a$ . Moreover, let  $m$  be any positive integer. Then we can always find  $m$  positive integers  $\mu^{(1)}, \mu^{(2)}, \dots, \mu^{(m)}$  such that for infinitely many integers  $\mu$  the  $2^m$  elements*

$a_\mu$					
$a_{\mu+\mu^{(1)}}$					
$a_{\mu+\mu^{(2)}}$	$a_{\mu+\mu^{(1)}+\mu^{(2)}}$				
$a_{\mu+\mu^{(3)}}$	$a_{\mu+\mu^{(1)}+\mu^{(3)}}$	$a_{\mu+\mu^{(2)}+\mu^{(3)}}$	$a_{\mu+\mu^{(1)}+\mu^{(2)}+\mu^{(3)}}$		
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\dots$	$\ddots$
$a_{\mu+\mu^{(m)}}$	$a_{\mu+\mu^{(1)}+\mu^{(m)}}$	$a_{\mu+\mu^{(2)}+\mu^{(m)}}$	$\dots$	$\dots$	$a_{\mu+\mu^{(1)}+\mu^{(2)}+\dots+\mu^{(m)}}$

are all equal to the same number  $G$ , where  $G$  is one of the numbers  $1, 2, \dots, a$ .

Thus we see that the statement *arises naturally from the necessity of proving that the coefficients of the negative powers of  $\sigma$  must be all equal to zero*. It is the strengthened form of the pigeonhole principle we mentioned earlier. It is stronger because it imposes a *structure* on the distribution of infinitely many common values  $a_s$  whereas the pigeonhole principle only implies their *existence*.

## 8 The Coefficients of the Negative Powers of $\sigma$ are Zero

Employing the above idea, we form the following  $m$  linear combinations:

$$\begin{aligned}\mathcal{P}^{(1)}(\sigma) &= \mathcal{P}(\sigma) - \mathcal{P}(\sigma + \mu^{(1)}) \\ \mathcal{P}^{(2)}(\sigma) &= \mathcal{P}^{(1)}(\sigma) - \mathcal{P}^{(1)}(\sigma + \mu^{(2)}) \\ &\vdots \\ \mathcal{P}^{(m)}(\sigma) &= \mathcal{P}^{(m-1)}(\sigma) - \mathcal{P}^{(m-1)}(\sigma + \mu^{(m)}).\end{aligned}$$

It follows from what we proved earlier that each of these  $m$  power series also assumes integer values for infinitely many integral arguments  $\sigma = \mu$ .

As we indicated, assuming the Cube Lemma, we obtain

$$\mathcal{P}^{(2)}(\sigma) = \varphi_{m-3}(\sigma) + \mu^{(1)}\mu^{(2)}v(v+1)\frac{B_{1v}}{\sigma^{v+2}} + \cdots,$$

where  $\varphi_{m-3}(\sigma)$  is a polynomial in  $\sigma$  of degree  $m-3$ . After  $m$  steps we arrive finally at the formula

$$\mathcal{P}^{(m)}(\sigma) = \mu^{(1)}\mu^{(2)} \cdots \mu^{(m)}v(v+1) \cdots (v+m-1)\frac{B_{1v}}{\sigma^{v+m}} + \cdots.$$

Since this power series begins with negative powers of  $\sigma$ , we can find a positive number  $\Gamma$  such that for all values of  $\sigma$  that exceed  $\Gamma$  the absolute value of the power series *will be smaller than one*. On the other hand, the power series  $\mathcal{P}^{(m)}(\sigma)$  is itself *equal to an integer for infinitely many arguments  $\sigma$*  and since an integer whose absolute value is less than one is necessarily equal to zero, it follows that *there are infinitely many integers  $\sigma$  for which the power series vanishes*.

But, our last formula shows us that

$$\lim_{\sigma \rightarrow \infty} [\sigma^{v+m}\mathcal{P}^{(m)}(\sigma)] = \mu^{(1)}\mu^{(2)} \cdots \mu^{(m)}v(v+1) \cdots (v+m-1)B_{1v},$$

where the expression on the right hand side represents a quantity *different from zero*. This last result stands in *contradiction* with the conclusion proven above, and therefore *it is impossible that a nonzero coefficient  $B_{1v}$  occurs among the coefficients  $B_{11}, B_{12}, B_{13}, \dots$* . It follows in the same way that *also the coefficients  $B_{2i}, B_{3i}, B_{4i}, \dots, B_{vi}$  must all be equal to zero*.

This completes the proof of the first conclusion about the Puiseux expansions of the coefficients of  $\pi_{as}(y, t)$ . ■

This step was the heart of Hilbert's proof and his paper's most brilliant insight. The other parts are clever too, but in our opinion this best shows his penetrating originality.

## 9 The Coefficients of the Polynomial Part are Rational Numbers

The next condition of Theorem 10 to be verified is: *the numerical coefficients in the polynomial part of the Puiseux expansions of the coefficients of  $\pi_{as}(y, t)$  are rational numbers*. Our

expansion has collapsed to the polynomial part:

$$\mathcal{P}(\sigma) = A_{11}\sigma^{m-1} + A_{12}\sigma^{m-2} + \cdots + A_{1m}, \quad (4)$$

where the right hand side assumes integer values for infinitely many values of  $\sigma$ . If we set the right hand side equal to these integers for  $m$  values of  $\sigma$  we obtain  $m$  linear equations with  $m$  unknowns  $A_{11}, A_{12}, \dots, A_{1m}$  which have a *rational solution* by Cramer's rule. This finishes the proof of the condition—we do not have to replace “rational” with “integral” because Proposition 7 showed that “rational” is enough. ■

## 10 Only Integral Powers of $t$

The final condition of Theorem 10 to be verified is: *the only non-zero terms in the polynomial part of the Puiseux expansions of the coefficients of  $\pi_{a_s}(y, t)$  are those with integral powers of  $t$ .*

Take  $\sigma$  to be a *prime* number  $p$  larger than  $C''$ .

We now determine  $2^n - 2$  distinct prime numbers  $p', p'', \dots, p^{2^n-2}$  all greater than  $p$ . Then also for each of these prime numbers there exists at least one among the  $2^n - 2$  formal factors whose coefficients have the above polynomial form (4). However, since the number of prime numbers  $p, p', p'', \dots, p^{2^n-2}$  is equal to  $2^n - 1$  while the number formal factors only reaches  $2^n - 2$ , necessarily *there must exist at least one formal factor admitting a double representation by these polynomials* (4). That is to say, as above:

$$\begin{aligned} y_1 + y_2 + \cdots + y_\nu &= A_{11}p^{-(m-1)/k}\tau_0^{m-1} + A_{12}p^{-(m-2)/k}\tau_0^{m-2} + \cdots + A_{1m} \\ &\vdots \\ y_1 y_2 \cdots y_\nu &= A_{\nu 1}p^{-(m-1)/k}\tau_0^{m-1} + A_{\nu 2}p^{-(m-2)/k}\tau_0^{m-2} + \cdots + A_{\nu m} \end{aligned}$$

and simultaneously

$$\begin{aligned} y_1 + y_2 + \cdots + y_\nu &= A'_{11}p'^{-(m-1)/k}\tau_0^{m-1} + A'_{12}p'^{-(m-2)/k}\tau_0^{m-2} + \cdots + A'_{1m} \\ &\vdots \\ y_1 y_2 \cdots y_\nu &= A'_{\nu 1}p'^{-(m-1)/k}\tau_0^{m-1} + A'_{\nu 2}p'^{-(m-2)/k}\tau_0^{m-2} + \cdots + A'_{\nu m}. \end{aligned}$$

If we equate coefficients of equal powers of  $\tau_0$  on the right hand sides we obtain:

$$\begin{aligned} A_{11}p^{-(m-1)/k} &= A'_{11}p'^{-(m-1)/k} & \dots = \dots & A_{1m}p^{-(m-1)/k} = A'_{1m}p'^{-(m-1)/k} \\ A_{21}p^{-(m-1)/k} &= A'_{21}p'^{-(m-1)/k} & \dots = \dots & A_{2m}p^{-(m-1)/k} = A'_{2m}p'^{-(m-1)/k} \\ \vdots &= \vdots & \dots = \dots & \vdots = \vdots \\ A_{\nu 1} &= A'_{\nu 1} & \dots = \dots & A_{\nu m} = A'_{\nu m} \end{aligned}$$

Since the coefficients  $A$ ,  $B$  and  $A'$ ,  $B'$  are all rational numbers and  $p$  and  $p'$  are distinct prime numbers, the above equations show us that *the only coefficients that can be different*

from zero are those for which the corresponding exponent of  $\tau_0$  must be an integer divisible by  $k$ , that is, the power series of our system are polynomials in  $\tau_0^k$  with rational coefficients, and if we put  $\tau_0^k = t_0$ , we obtain:

$$\begin{aligned} y_1 + y_2 + \cdots + y_\nu &= F_1(t_0) \\ \vdots & \quad \quad \quad \vdots \\ y_1 y_2 \cdots y_\nu &= F_\nu(t_0), \end{aligned}$$

where  $F_1(t_0), \dots, F_\nu(t_0)$  are polynomials in  $t_0$  with rational coefficients.

This completes the proof of the third property of the Puiseux expansions of the coefficients of  $\pi_{a_s}(y, t)$ . ■

We have shown that the formal factor  $\pi_{a_s}$  fulfills the three conditions of **Theorem 10** and therefore the proof of our theorem is complete. ■

## 11 Later Proofs of the Irreducibility Theorem

Virtually all modern proofs of the (two-variable) irreducibility theorem are based on that of Dorge [4], which sharpened an idea of Skolem [24]. The latter's clever strategy is the following: Assume that  $f(x, t)$  is irreducible for infinitely many integral values  $t_k$  of  $t$ . Form, as does Hilbert, the formal factors of  $f(x, t_k)$  for some fixed  $k$ . Then *no formal factor can be an integral polynomial in  $x$* . That means that at least one Puiseux expansion at infinity of the coefficients of any formal factor cannot collapse down to an integral polynomial in  $t$ , for if they all do, then that formal factor is an integral polynomial in  $x$  which contradicts the assumption. So, every formal factor has at least one coefficient Puiseux series which does not collapse down to an integral polynomial in  $t$ . Let  $\varphi_1(t), \dots, \varphi_N(t)$  be these Puiseux series, one taken from each formal factor.

Thenceforth, to prove Hilbert's theorem it suffices to prove that *there are infinitely many integers  $t_k^*$  such that the  $N$  Puiseux series  $\varphi_1(t_k^*), \dots, \varphi_N(t_k^*)$  are all simultaneously irrational*. Then each formal factor of  $f(x, t_k^*)$  will have an irrational coefficient and  $f(x, t_k^*)$  will be irreducible over the integers.

Therefore one is led to investigate those integers for which a non-polynomial Puiseux series takes on integer values. Skolem showed that *the density of such integers in the set of all integers is zero*. That is, if  $x_1 < x_2 < \cdots < x_k < \cdots$  are the integers where the non-polynomial Puiseux series takes on integer values, then Skolem proved:

$$\lim_{k \rightarrow \infty} \frac{k}{x_k} = 0.$$

We have glossed over many details. For example it is sufficient to consider Puiseux series at infinity that do not collapse down to polynomials with *rational* coefficients. Although the integers  $x_k$  where the series takes on integral values have density zero, what about the density of integers where they take *rational* values? This too is zero. We refer the reader to [16, 17, 18] for details.

The two approaches, Hilbert's and Skolem's, are completely different. They both use the formal factor factorization and they both use the Puiseux expansions at infinity of the coefficients. But Hilbert's, proving the contrapositive, seeks an integral polynomial factor (and finds one) whereas Skolem's seeks to find integers for which a finite set of Puiseux series are all irrational (and finds them). The latter approach is number theoretical and uses the fundamental ideas of Diophantine approximation.

All modern work has focused on quantitative estimates of the density  $k/x_k$  of the integers with integral-valued Puiseux expansions at infinity. For examples we again point the reader to the above references.

## 12 Hilbert Cube Numbers and Conclusions

Define the "Hilbert Cube Number"  $H(m, c)$  to be the *least* number  $H$  such that every  $c$ -coloring of  $1, \dots, H$  has a monochromatic  $m$ -cube. Our proof of the Cube Lemma in Section 2 showed a recursive upper bound  $H(m, c) \leq H(m-1, c)(1 + c^{H(m-1, c)})$ , with basis  $H(1, c) = 1$  for all  $c$ . This is far from best possible. For one thing, when  $2 \leq m \leq c$  one can improve the upper bound to  $H(m, c) \leq h(1 + c(m-1)^h)$  where  $h = H(m-1, c)$  by a different counting argument. One can further tweak this with  $\binom{m-1}{h}$  in place of  $(m-1)^h$ . These formulas are not bounded by any fixed tower of exponents in  $c$  and  $m$ .

As observed by Brown et al. [2], Hilbert's original proof yields bounds with  $(c+1)$  rather than  $(m-1)$  in the base and the Fibonacci number  $F_{2m}$  in the exponent. Namely,  $H(m, c) \leq (c+1)^{F_{2m}}$ , where  $F_0 = 0, F_1 = 1, F_2 = 1, F_3 = 2, \dots$ . These bounds have double-exponential growth. Szemerédi [26] (see also [9]) improved both the bounds and the nature of the result, showing that any subset  $A$  of  $[1, \dots, H]$  of density  $1/c$  (that is,  $|A| \geq H/c$ ) contains an  $m$ -cube where  $m \geq \log \log(H) - C$  and  $C$  depends only on  $c$ . The best known upper and lower bounds appear still to be those of Gunderson and Rödl [10]:

$$c^{(1-\epsilon_c)(2^m-1)/m} \leq H(m, c) \leq (2c)^{2^{m-1}},$$

where  $\epsilon_c \rightarrow 0$  as  $c \rightarrow \infty$ . The same upper bound was recently ascribed to [11] by Conlon, Fox, and Sudakov [3] but see also Sándor [22] with different asymptotics. Erdős and Turán [5] proved that  $H(2, c)$  is asymptotic to  $c^2$ , but the remarks in [2] that less is known about  $H(m, c)$  for fixed  $m \geq 3$  appear still in force, and [3] remarks that  $H(m, 2)$  depends on unknown properties of van der Waerden numbers.

We have shown the significance of the Cube Lemma in the context of Hilbert's original paper. The question of whether Hilbert might have expanded on it bids comparison with Ramsey's motivation in [21]. That was a problem in logic not number theory *per se*. But Hilbert was the world's master in the relationship between number theory and logic until Gödel emerged, so one may ask again why Hilbert didn't pursue this further or develop areas of extremal combinatorics *vis-à-vis* logic in the direction of Ramsey theory. We close with a speculative answer: the world in which Hilbert was immersed is as different from that of Ramsey Theory as "doubly-exponential" is from "singly-exponential."



The years 1890–1893 saw the publication of Hilbert’s great foundational works in commutative algebra, including his Basis Theorem and *Nullstellensatz* [12, 14]. A common thread through all this work is the notion of *regularity*: given a finitely-specified system of elements that may have arbitrarily large values of some parameter  $t$  (such as the degree of polynomials over a ring), there is some integer  $t_0$  such that for all  $t \geq t_0$  the system conforms to a simple description. Hilbert first proved his Basis Theorem non-constructively. Later was it shown that the growth of the relevant  $t_0$  (in terms of the degrees  $d$  of basis elements or the  $n$ -variable equations in the *Nullstellensatz*) is double-exponential, of order at most  $d^{2^n}$ . Our answer to the question we posed in the previous paragraph is that Hilbert was simply occupied with more-rarefied levels of algebra and analysis revolving around invariants. Irreducibility of polynomials plays into irreducible varieties and primary decompositions of polynomial ideals, which Hilbert’s student Emanuel Lasker (the world chess champion) and protégé Emmy Noether built upon for some great work in the next two decades. Meanwhile, Hilbert swooped down to the utterly ground-level task of formalizing Euclid’s geometry in the later 1890s, which presaged his work on formal systems of logic.

The divide in purpose and growth rate doesn’t ward us off from appreciating the cube numbers and seeking other uses for them. That is why we have devoted this paper to expounding their original use and context. We have highlighted how the Cube Lemma completed an insight about estimates by infinite series. We hope that our exposition will foster a greater appreciation of combinatorial underpinnings of more “analytical” areas of mathematics.

**Acknowledgements** The first author acknowledges support by the Vicerectoria de Investigación from the University of Costa Rica. We thank Umberto Zannier for calling our attention to the role of Gauss’s Lemma in section 3.

## References

- [1] M. Bôcher. *Introduction to Higher Algebra*. Dover, New York, 2004.
- [2] T. C. Brown, F. R. K. Chung, P. Erdős, R. L. Graham. Quantitative forms of a theorem of Hilbert. *J. Combin. Theory Ser. A* **38** (1985) 210–216.
- [3] D. Conlon, J. Fox, B. Sudakov. Short proofs of some extremal results. *Combin. Probab. Comput.* **23** (2014) 8–28.
- [4] K. Dörge. Einfacher Beweis des Hilbertschen Irreduzibilitätssatzes. *Math. Ann.* **96** (1927) 176–182.
- [5] P. Erdős and P. Turán. On a problem of Sidon in additive number theory, and on some related problems. *J. London Math. Soc.* 16 (1941) 212–215.
- [6] W. Franz. Untersuchungen zum Hilbertschen Irreduzibilitätssatz. *Math. Z.* **33** (1931) 275–293.

- [7] D. Fried. On Hilbert's irreducibility theorem. *J. Number Theory* **6** (1974) 211–231.
- [8] Carl Friedrich Gauss *Disquisitiones Arithmeticae* tr. Arthur A. Clarke. Yale Univ Press, New York, 1965.
- [9] R. Graham, B. Rothschild, J. Spencer. *Ramsey Theory*. Wiley, New York, 1990.
- [10] D. S. Gunderson, V. Rödl. Extremal problems for affine cubes of integers. *Combin. Probab. Comput.* **7** (1998) 65–79.
- [11] D. S. Gunderson, V. Rödl, A. Sidorenko. Extremal problems for sets forming Boolean algebras and complete partite hypergraphs. *J. Combin. Theory Ser. A* **88** (1999) 342–367.
- [12] D. Hilbert. Über die Theorie der algebraischen Formen. *Math. Ann.* **36** (1890) 473–534.
- [13] D. Hilbert. Über die Irreducibilität ganzer rationaler Functionen mit ganzzahligen Coefficienten. *J. reine angew. Math.* **110** (1892) 104–129.
- [14] D. Hilbert. Über die vollen Invariantensysteme. *Math. Ann.* **42** (1893) 313–373.
- [15] B. Landman, A. Robertson. *Ramsey Theory on the Integers*. AMS, Providence, 2004.
- [16] S. Lang. *Diophantine Geometry*. Wiley, New York, 1962.
- [17] S. Lang. *Fundamentals of Diophantine Geometry*. Springer, New York, 1983.
- [18] K. Nowak. Some elementary proofs of Puiseux's theorems. *Univ. Iagel. Acta Math.* **38** (2000) 279–282.
- [19] V. Prasolov. *Polynomials*. Springer, New York, 2004.
- [20] H. J. Promel. *Ramsey Theory for Discrete Structures*. Springer, New York, 2013.
- [21] F. P. Ramsey. On a problem in formal logic. *Proc. London Math. Soc.* **30** (1930) 264–286.
- [22] C. Sándor. An upper bound for Hilbert cubes. *J. Combin. Theory Ser. A* **114** (2007) 1157–1159.
- [23] A. Schinzel. *Selected Topics on Polynomials*. Univ. of Michigan Press, Ann Arbor, 1982.
- [24] T. Skolem. Untersuchungen über die moeglichen Verteilungen ganzzahliger Lösungen gewisser Gleichungen. *Kristiania Vid. Selsk. Skr.* **17**, 1921; 57 pp.
- [25] A. Soifer. *The Mathematical Coloring Book: Mathematics of coloring and the colorful life of its creators*. Springer, Berlin, 2009.
- [26] E. Szemerédi. On sets of integers containing no four elements in arithmetic progression. *Acta. Math. Hungar.* **20** (1969) 89–104.
- [27] N. Tzanakos. *Elliptic Diophantine Equations*. De Gruyter, Berlin, 2013.